Security considerations on extending PACE to a biometric-based connection establishment

Nicolas Buchmann*, Roel Peeters†, Harald Baier* and Andreas Pashalidis†

*da/sec Biometrics and Internet Security Research Group
Hochschule Darmstadt, Darmstadt, Germany
firstname.lastname@h-da.de

†KU LEUVEN, ESAT/COSIC & iMinds, Belgium
firstname.lastname@esat.kuleuven.be

Abstract: The regulations of the European Union (EU) Council in 2004 are the basis of the deployment of electronic passports within the EU. Since then EU member states adopt the format and the access protocols to further electronic machine readable travel documents (eMRTD) like national electronic ID cards and electronic residence permits, respectively. The security protocols to communicate with an eMRTD are based on the paradigm of strong cohesion and loose coupling, i.e., each step is designed to ensure only a particular security goal like authorisation to access a certain data group, authenticity and integrity of the data, originality of the chip, or the linkage between the eMRTD and its holder. However, recently a discussion evolved to integrate the linkage security goal within the connection establishment, which currently only aims at limiting basic access of authorised terminals to the eMRTD. For instance, the BioPACE protocol proposes to replace the knowledge-based shared 'secret' of PACE by a biometric-based one. The goal of the paper at hand is twofold: First, we evaluate the BioPACE protocol and propose improvements to enhance its features. Second, we analyse the expediency of integrating our BioPACE version 2 into the eMRTD domain. Our initial evaluation shows that our BioPACE version 2 is expedient if the EAC protocols and the corresponding PKI are abandoned.

1 Introduction

Since 2004 EU member states issue ePassports, which feature an embedded radio frequency (RF) chip [EU04, EU05]. This chip contains sensitive biometric data, typically including the ePassport holder's facial image and fingerprints of two index fingers [ICA06]. In order to address the risks that arise through the electronic storage and wireless communication channel, security protocols for ePassports have been specified [ICA06, BSI10]. The privacy of ePassport holders, for example, is protected by access control mechanisms, which ensure that only trusted parties may read the fingerprints. Confidentiality of the transferred data is achieved by encrypting all communication between an inspection system and the chip. The specified protocols also ensure authenticity and integrity of the data read from the chip, as well as the originality of the chip itself.

The specified security protocols follow the paradigm of strong cohesion and loose coupling. That is, each protocol fulfils a very specific security goal and the security protocols hardly depend on each other, if there is a dependency at all. This paradigm is well established in the software engineering community [IEE90, ISO05].

Due to this principle further chip equipped cards (e.g., electronic ID cards) with similar security goals can use a subset of the ePassports' security protocols and replace an ePassport protocol by a new one where appropriate. This does not only create a benefit for the electronic ID cards, but instead a mutual gain, because if a new improved security protocol is favoured in the electronic ID card domain it might replace the ePassport counterpart in the long term. This is currently the case for the Password Authenticated Connection Establishment (PACE, [BSI10]), which is expected to replace the Basic Access Control (BAC) protocol by the PACE-based Supplemental Access Control (SAC) in 2018 [ICA13].

Recently Deufel et al. [DMDK13] propose the BioPACE protocol as a replacement for the knowledge-based shared 'secret' of PACE. The BioPACE protocol uses a biometric-based secret instead.

The goal of our paper is twofold: Firstly, we evaluate the BioPACE protocol. We document weaknesses compared to PACE, especially that BioPACE enables tracking and abandons the connection of the physical document and its chip. Additionally we propose improvements to enhance its features. Secondly, we analyse the expediency of integrating our BioPACE version 2 into the eMRTD domain. We sketch the idea of replacing the expensive Extended Access Control (EAC) protocols and its related Country Verifying Public Key Infrastructure (CV PKI) by our BioPACE version 2 protocol. An initial evaluation reveals that our BioPACE version 2 actually has the potential to serve as replacement, if some of the conveniences of EAC are considered to be dispensable (e.g., fine-grained authorisation levels to different data groups).

This paper is organised as follows: Section 2 describes the security protocols, which are relevant for the later discussion of BioPACE. In Section 3 the concept and underlying idea of BioPACE is introduced. The security assessment of BioPACE is presented in Section 4. Section 5 proposes an enhanced version of BioPACE. Section 6 presents future plans to replace EAC with our BioPACE version 2, and discusses the expediency of our BioPACE version 2 in the eMRTD domain. In Section 7 conclusions are drawn and the presented improvements and the usefulness of BioPACE are discussed.

2 eMRTD protocols and their security goals

This section describes the eMRTD protocols and their security goals. Each protocol fulfils a very specific security goal. The protocols are either specified by the International Civil Aviation Organisation (ICAO) [ICA06] or the German Federal Office for Information Security (BSI) [BSI10], and are well described in [KN07].

Passive Authentication is the only protocol, which is specified as mandatory by the ICAO [ICA06]. It provides authenticity and integrity of the data stored on the chip. Passive Authentication depends on the so-called *Signing PKI*.

Basic Access Control (BAC) provides protection against unauthorised access to the data stored on the chip [ICA06]. Unauthorised means access to the data without the eMRTD owner handing over the document. To get access to the chip the terminal needs optical access to the data page to read the Machine Readable Zone (MRZ). The terminal authenticates itself to the chip with the data read from the MRZ, and both entities agree on session keys during BAC to establish a secure channel which provides authenticity, integrity and confidentiality of the transferred data by means of the *Secure Messaging* sub-protocol.

To protect the sensitive data groups BAC is not sufficient. Therefore *Extended Access Control* (EAC) protects data group 3 (DG3), which contains the fingerprints. EAC consists of *Terminal Authentication* and *Chip Authentication* [BSI10]. After performing EAC the terminal can read the fingerprints, capture a biometric sample from the eMRTD holder and compare the biometric data to check if the current eMRTD holder is the legitimate owner, and thereby achieves the linkage security goal.

To prevent chip cloning, two protocols exist in the eMRTD domain. *Active Authentication* (AA) specified by the ICAO [ICA06] and as part of EAC *Chip Authentication* (CA) specified by the BSI [BSI10]. Both protocols prove the authenticity of the chip (originality) to the terminal. AA achieves this goal with a challenge-response protocol and CA establishes a strong secure channel based on the Diffie-Hellman protocol to implicitly prove the originality of the chip.

Terminal Authentication (TA) is part of EAC and is a protocol by which a terminal can prove to a chip its access right to the sensitive biometric data [BSI10]. The chip forces every terminal to prove its authorisation to DG3 before granting access to the fingerprints. TA is based on a PKI for terminals called the *Country Verifying PKI*.

The *Password Authenticated Connection Establishment* (PACE) fulfils the same security goals as BAC, but provides strong session keys even in the presence of low-entropy passwords, and contrary to BAC is resistant against offline brute-force attacks [BSI10]. The shared password is denoted by π and can either be received from the MRZ, a PIN, or the Card Access Number (CAN), which is printed on the data page of the eMRTD and consists of a six digit number. PACE is based on symmetric and asymmetric cryptography, while BAC is based solely on symmetric cryptography. PACE is depicted in Figure 1 and roughly consists of the following steps:

- First the eMRTD chip randomly chooses a nonce s and encrypts it with K_π which is derived from the shared password π. The chips sends the ciphertext $z = Enc_{K_\pi}(s)$ to the terminal.
- The terminal recovers s with the shared password π and receives $s = Dec_{K_\pi}(z)$.
- Chip and terminal both create ephemeral key pairs, and perform a Diffie-Hellman key agreement protocol based on these key pairs and the generated shared secret s. By performing Diffie-Hellman both entities agree on a new shared secret K.
- Based on K both parties derive session keys.
- Chip and terminal exchange and verify authentication tokens based on a Message Authentication Code.

- After successfully performing PACE the *Secure Messaging* sub-protocol is started with the derived session keys to establish a secure channel, which provides authenticity, integrity and confidentiality.

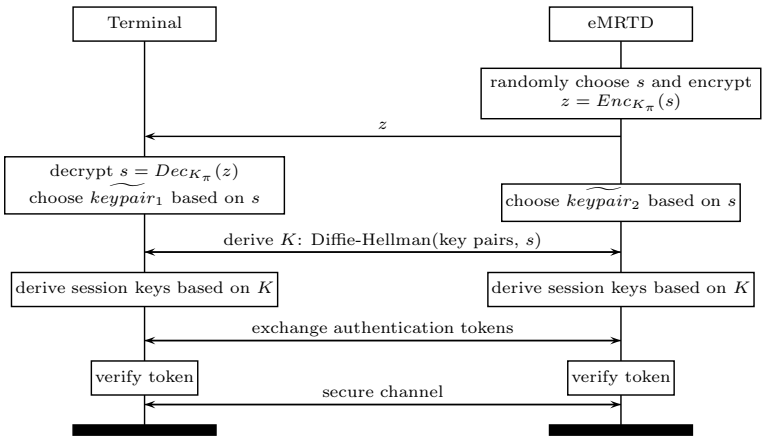

Figure 1: The PACE protocol

PACE is the basic building block for the BioPACE protocol introduced in the next section.

3 BioPACE

This section presents the BioPACE security protocol and its underlying idea as introduced by Deufel et al. in [DMDK13]. Deufel et al. present BioPACE as a pre-processing step to the PACE protocol, which we describe in Section 2. We first sketch the idea of BioPACE and then describe its two phases.

The underlying idea for the pre-processing step is to make use of biometric template protection based on the ISO/IEC 24745 standard for biometric information protection [ISO11]. BioPACE does not favour a biometric modality, i.e., BioPACE may be implemented using the facial image, fingerprints, iris, etc. During personalisation of an eMRTD the biometric modality is enrolled and a feature extraction from the captured biometric sample results in a biometric reference comprising of a pseudonymous identifier PI and auxiliary data AD. The concrete specification of PI and AD with respect to size and structure is neither specified by the ISO/IEC 24745 standard nor by the authors of [DMDK13]. A verification consists of a new feature extraction from a fresh biometric sample and the previously enrolled AD. The verification results in a new pseudonymous identifier PI^*, which equals PI if and only if the same person provided the biometric sample and therefore a biometric match occurs.

We now explain the two phases of BioPACE in more detail. The authors of [DMDK13] call these phases the *initialisation phase* and the *regular use phase*.

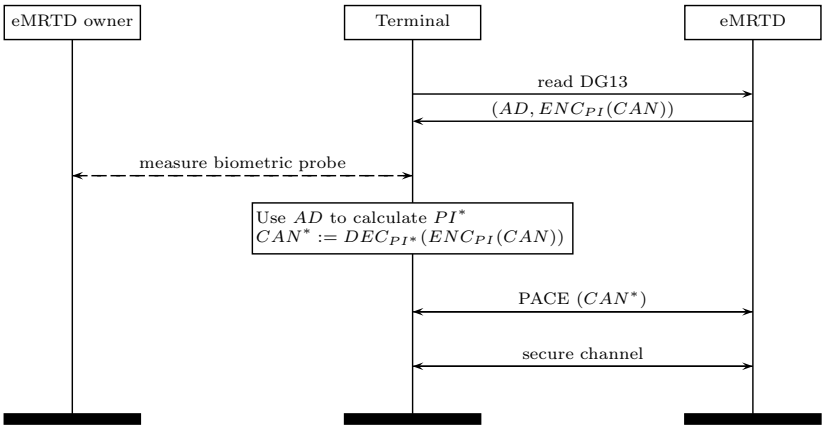

Figure 2: The BioPACE protocol

During the initialisation phase the biometric enrolment is conducted, which results in PI and AD. Additionally the eMRTD chip or a backend system creates a random CAN or PIN, which serve as input for the regular PACE protocol after the pre-processing step of BioPACE. In what follows we denote this random secret as CAN. The secret CAN is encrypted using PI as encryption key resulting in $ENC_{PI}(CAN)$. Then PI is discarded. The pair $(AD, ENC_{PI}(CAN))$ is then written to data group 13 (DG13) of the eMRTD logical data structure (LDS) [ICA06]. DG13 is publicly accessible without any authentication. This is justified by [DMDK13] with the consideration that the tuple $(AD, ENC_{PI}(CAN))$ is not security sensitive, because it does not disclose biometric data of the enrolled person.

After the initialisation phase BioPACE is ready for regular use. This phase is depicted in Figure 2. If an inspection system wants to perform BioPACE, it first has to read DG13 to receive $(AD, ENC_{PI}(CAN))$. The inspection system captures a biometric sample from the document holder and uses the received AD from DG13 to compute PI^*. The inspection system then performs $DEC_{PI^*}(ENC_{PI}(CAN))$ to decrypt $ENC_{PI}(CAN)$ using PI^* as decryption key to receive CAN^*, which will match CAN if and only if PI^* matches PI.

The secret value CAN is also known to the eMRTD chip, because it is stored in its internal memory and can therefore be used as input for the standard PACE protocol. After this pre-processing step BioPACE uses the steps of the PACE protocol, which we explain in Section 2.

4 Assessment of BioPACE

In this section we present our security assessment of BioPACE with respect to common security features of an eMRTD. We identified weaknesses that are introduced when replacing PACE with BioPACE. Every paragraph first presents a short assessment regarding

a specific security aspect, and then proposes possible solutions, when applicable.

No physical to electronic linkage. Where PACE makes a link between the printed data page of the eMRTD and the chip inside the eMRTD, BioPACE makes a link between the eMRTD owner and the chip inside the eMRTD. There is no link anymore between the printed data page of the eMRTD and the chip inside the eMRTD. As a consequence it cannot build further upon the prior established authenticity of the MRZ and CAN (by checking the optical security features on eMRTDs, such as special paper and printing techniques).

Tracking. While PACE guarantees the unlinkability of eMRTD occurrences on the wireless channel, BioPACE does not. The authors of BioPACE justify that data group 13 can be read freely from the chip by claiming that it does not disclose any biometric data and as such is not security-sensitive. However, the data $(AD, ENC_{PI}(CAN))$ provides a unique identifier for every eMRTD and can be read out by anyone within communication range of the eMRTD making tracking possible.

A possible solution would be to print $(AD, ENC_{PI}(CAN))$ on the data page of the eMRTD, additionally ensuring the coupling between the data page of the eMRTD and the chip. However, this would require substantial changes in the eMRTD creation and verification processes, as opposed to reading out some extra values from the chip.

Usability degradation. The aspect of better comfort is not proven in the paper. We doubt that reading and processing a fingerprint is faster than performing OCR on a MRZ or CAN. Implementing BioPACE instead of PACE also means that the verifier needs biometric reader equipment, even if one only wants to read the chip's version of the holder's name, or to verify authenticity and integrity of the chip's data via passive authentication. At the end of the paper, it is suggested that one can always skip the biometric pre-processing step of BioPACE and fall back to the original PACE. However, if the biometric pre-processing step can be skipped, this raises questions about the benefits of BioPACE, especially towards the eMRTD owner.

Loss of access control flexibility. As long as the sensitive biometric fingerprints are stored on the chip BioPACE should not be considered as EU EAC replacement, because it can only provide two possible authorisation levels: read every data group or read no data group. With EAC, one can provide a more fine grained access control and the eMRTD receives an explicit authorisation from its issuing country that this terminal is indeed authorised to read certain data groups.

A possible solution is to replace the raw fingerprints by a biometric template that leaks no sensitive information.

Double biometric linkage goal. The basic BioPACE protocol claims to provide access control and create a link between the eMRTD holder and the chip. In the current eMRTD security protocol pool these goals are already achieved by BAC, PACE and EAC for the access control and the fingerprints stored on the chip for the biometric link. Achieving the same security goal twice has no benefit and only makes the border control check more lengthy.

Removing EAC and the raw fingerprints would justify the access control and linkage goal of BioPACE. Of course this should only be considered if the eMRTD would contain no more sensitive biometric data.

Skimming. BioPACE claims that no unauthorised data retrieval is possible. For eMRTDs that implement PACE, one requires access to the printed data page of the eMRTD to read the data on the chip. Handing the eMRTD over to an official for checking can be seen as an implicit authorisation from the eMRTD owner. For BioPACE to reach the same level of authorisation, eMRTD holders can only provide their fingerprint to the officials checking their eMRTDs. However, we leave our fingerprints everywhere. Anyone within wireless communication range that has access to the fingerprint of the eMRTD holder, can read out the data of the eMRTD without the owner even being aware. This makes skimming attacks easy, for example in airport bars (given that one can extract the fingerprint from a glass in a timely manner). One does not need to fool the terminal's fingerprint reader (which is hard, since one has to make a dummy finger, possible liveness detection) but the raw image data is good enough for direct processing. As boundary condition, the attacker also needs a terminal and the attack is only justified if a name or facial image to a corresponding fingerprint is the goal of the attacker.

By making a link to the printed data page of the eMRTD this attack can be mitigated, because the printed content is not revealed in airport bars.

Offline eMRTD owner guessing. Because the CAN has low entropy, an offline guessing attack with respect to whom the eMRTD belongs to is possible. Assume that one wants to track a number of high profile individuals and one has access to their fingerprints (which are left behind on whatever the person in question happens to touch). From these fingerprints, together with AD one can derive all possible PI's. Only a subset of the corresponding $ENC_{PI}(CAN)$ will decrypt to a possible CAN (having low entropy). Of course this will not uniquely identify any one person, but it will narrow down the search space significantly.

A trivial solution would be to pad the CAN with some randomness before encryption, and discard the padding upon decryption. Note that this would not work, when using the MRZ instead of the CAN. While the MRZ has typically more entropy than the CAN, it also has more structure that is preserved regardless of the random padding.

A side note worth mentioning: If PI could provide a high enough entropy it could also make BAC attractive again, because the main complaint of BAC is the low entropy of the MRZ combined with its vulnerability to offline brute-force attacks. Still PACE is resistant against offline brute-force attacks and should therefore preferred over BAC.

5 An improved BioPACE: BioPACE version 2

This section formalises our BioPACE version 2 protocol. It aims at fixing the flaws identified in Section 4 by changing BioPACE according to the proposals of Section 4.

Figure 3 on the next page illustrates the protocol steps of our BioPACE version 2 protocol.

The improvement consists of two main changes compared to the basic version: First, PI^* is used directly as input for the PACE protocol (and not as decryption key to get the low entropy CAN). Second, AD is printed on the data page of the eMRTD to link the physical document to the chip instead of storing AD on the chip.

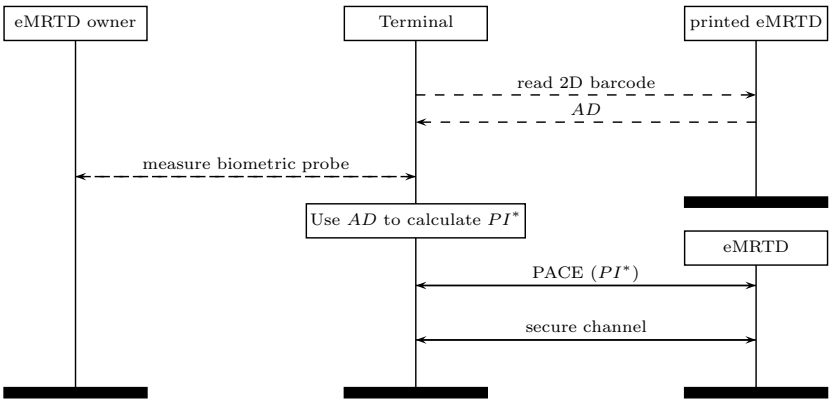

Figure 3: Our BioPACE version 2 protocol

We see no reason why one should encrypt a low entropy value (CAN or MRZ) if it does not need to be transferred manually/optically. Therefore, we use PI^* directly as input for the PACE protocol. This also means that the value $ENC_{PI}(CAN)$ no longer needs to be transmitted from the eMRTD to the terminal via the wireless channel. Hence there is no initial access from the terminal to DG13 of the eMRTD. By removing the initial wireless access we avoid the issue of offline guessing of the eMRTD owner, too.

AD is printed on the data page of the eMRTD in form of a 2D barcode (e.g., a QR code [ISO06b] or a Data Matrix code [ISO06a]), which is shown in Figure 4 on the following page. PI is not publicly available, instead it is stored in the internal memory of the eMRTD chip and therefore only available to the chip itself, but not to the terminal. Since the chip does not need to transmit $(AD, ENC_{PI}(CAN))$, there is no longer a unique identifier for the eMRTD, resolving the tracking problem.

We decided against integrating AD into the present MRZ, because in our experience a 2D barcode is more reliable due to the integrated error correction code and more flexible for an AD with variable size depending on the selected biometric modality. 2D barcodes become more and more popular in different areas of document security.

For instance, there is currently a discussion in the EU to integrate 2D barcodes to enhance the authenticity and integrity of non-electronic travel and ID documents (e.g., birth certificates, emergency passports, visas and driver licenses). This EU discussion is based on a new national standard, which is called the Digital Seal [BSI13].

By printing AD on the data page we recreate the link between the physical eMRTD and the chip. Now a terminal needs optical access to the eMRTD to scan the 2D barcode and receive AD to calculate PI^*. This will provide at least the same level of protection against skimming and sniffing attacks as PACE.

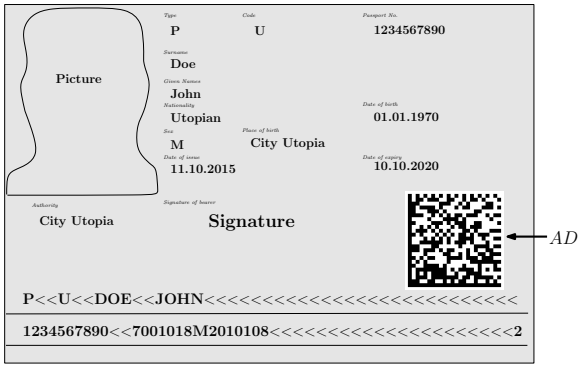

Figure 4: The eMRTD data page with AD printed as data matrix code

In the basic BioPACE protocol, matching PI to PI^* is done implicitly by decrypting the low-entropy CAN with PI^* and initialising PACE with the resulting CAN^*. The key space entropy of PI is not specified by [DMDK13], but we consider it higher than the entropy of a numeric six digit CAN with an entropy of at most 20 bits. Therefore we directly enter PI^* into PACE. Besides the higher entropy benefit, PI^* is implicitly matched to PI by the completion of the PACE protocol, because if PI^* and PI do not match the PACE protocol will fail.

Our BioPACE version 2 fixes all the mentioned security problems of Section 4. Now, it fulfils its duty as an access control mechanism and leaks no more unambiguous linkable data before the protocol successfully completes. To track a person and to read the data on the chip the attacker needs optical access to the data page. This equals the current security level of eMRTDs and does not constitute a security risk, because if an attacker gets access to the data page he can read all data in printed form anyway.

Still some problems remain and therefore we will discuss the expediency of our BioPACE version 2 in the eMRTD domain in the subsequent section.

6 Replacing EAC and raw fingerprints by BioPACE version 2

In this section we discuss our idea to replace the current infrastructure (i.e., the EAC protocols, the Country Verifying PKI, and the storage of raw fingerprints in data group 3) by our BioPACE version 2 protocol. We contrast the advantages with the disadvantages of our approach and include boundary conditions, which have to be fulfilled to make our BioPACE version 2 expedient.

Fundamental changes to an established infrastructure are a challenging task and require as a boundary condition both innovative ideas and enhanced security. We consider BioPACE version 2 to meet these demands as discussed below. In our context, for instance, a sample innovative idea is the Biocryptographic Key Infrastructure [SBB10] to replace a common

Public Key Infrastructure, yielding a higher security level. An example of enhancing an applied and proven protocol is the Biotokens [SB08] example, where biometric digital signatures and Bio-Kerberos increases security. Therefore the redundant protocols have to be dropped, and the BioPACE version 2 has to provide a significant enhancement to become a new eMRTD standard.

If BioPACE version 2 is used without a subsequent EAC accomplishment, we see the following benefits:

1. **Faster verification:** If we drop EAC and make use of a PI instead of raw fingerprints, we eliminate two bottlenecks: first, no more raw fingerprints have to be transferred from the chip to the terminal over the wireless interface. Second the lack of terminal authentication resolves the need to verify certificate chains by the eMRTD chip. This will drastically speed up the eMRTD processing times at border checks.
2. **Enhanced practical security:** According to a recent EU border control study [Com, D4.1] border control personnel does only perform an electronic check against eMRTD blacklists due to time constraints. Hence in practice the actual security level of the eMRTD chip and its infrastructure is mainly not used. A significant speed-up of the verification protocols will therefore not only make the verification more convenient for the travellers, but it will improve security, because the electronic security features will be actually used by border control personnel even under strict time schedule guidelines.
3. **Improving privacy:** Raw fingerprints are removed and replaced with a biometric template, which is stored in the eMRTD's internal memory and therefore only accessible by the chip. Hence the privacy level is improved.
4. **Decreasing infrastructure costs:** If we abandon terminal authentication, there is no more need to maintain the complicated Country Verifying PKI. As the further expenses remain constant (e.g., the costs for the biometric personalisation of eMRTDs), the costs of the whole eMRTD infrastructure will decrease significantly.
5. **Standardised data structures:** 2D barcodes are standardised, and their integration is already discussed for non-electronic travel documents based on the Digital Seal standard [BSI13, Com, D6.1].

On the other hand BioPACE version 2 as a replacement for EAC yields the following downsides:

1. **Change of layout:** To establish the BioPACE version 2 protocol in the eMRTD domain the creation and enrolment process has to be changed, because AD needs to be printed on the data page.
2. **Coarse-grained access control:** As discussed in Section 4 BioPACE version 2 causes a loss of access control flexibility. However, if the sensitive JPEG fingerprints are removed from the chip no more sensitive data remains, which is worth protection with a flexible access control scheme.

3. **Renounce of strong cohesion paradigm:** Security protocols often follow the software engineering paradigm of strong cohesion and loose coupling. Every protocol should have a very specific goal and depend on as few as possible other protocols. Our proposal abandons this paradigm.

4. **Chip cloning:** Dropping EAC results in the loss of chip authentication and hence in giving up the current chip cloning protection. However, the physical protection through the printed AD on the document makes chip cloning useless from a practical point of view. We discuss a further electronic prevention approach of chip cloning below.

To conclude we rate the improvement with respect to run-time, practical security, and costs to be more important than the disadvantages to change the layout and the loss of fine-grained access control.

Future attention should be paid to a sample specification of the PI scheme and to the integration of a chip cloning protection into the BioPACE version 2 protocol. Bender et al. [BDFK12] present a protocol called PACE|AA, which combines PACE and Active Authentication to create a protocol, which is more efficient than the single protocols and solves a security risk of Active Authentication.

7 Conclusion and future work

This paper presented an assessment of the BioPACE protocol, pointed out flaws in the basic version and proposed an optimised version which fixed these flaws. The second part of this paper analysed the expediency of the BioPACE version 2 protocol and came to the conclusion that it is not expedient in its proposed form. The final section presented a drastic approach which makes our BioPACE version 2 very attractive if the EAC protocols together with the expensive CV PKI are shut down and our BioPACE version 2 gets merged with the PACE|AA protocol to also get a chip cloning protection and become a perfectly tailored monolithic security protocol for the eMRTD domains requirements.

We presented the theoretical idea of merging our BioPACE version 2 protocol with the PACE|AA protocol, therefore future work will focus on a formal security proof for this protocol based on the model proposed by Bellare et al.[BPR00].

Acknowledgement

This work was supported by the European Commission through the FIDELITY EU-FP7 project (Grant No. SEC-2011-284862), CASED and the Research Council KU Leuven: GOA TENSE (GOA/11/007).

References

[BDFK12] Jens Bender, Özgür Dagdelen, Marc Fischlin, and Dennis Kügler. The PACE|AA Protocol for Machine Readable Travel Documents, and Its Security. In *Financial Cryptography and Data Security*, volume 7397 of *LNCS*, pages 344–358. Springer, 2012.

[BPR00] Mihir Bellare, David Pointcheval, and Phillip Rogaway. Authenticated Key Exchange Secure against Dictionary Attacks. In *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 139–155. Springer, 2000.

[BSI10] BSI. *Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*. Bundesamt für Sicherheit in der Informationstechnik (BSI), 2.05 edition, 2010.

[BSI13] BSI. *Technical Guideline TR-03137 Optically Verifiable Cryptographic Protection of non-electronic Documents (Digital Seal)*. Bundesamt für Sicherheit in der Informationstechnik (BSI), 1.0 edition, 2013.

[Com] European Commission. FIDELITY Project. online, http://www.fidelity-project.eu/page/project/deliverables.php.

[DMDK13] Bernhard Deufel, Carsten Mueller, Gavan Duffy, and Tom Kevenaar. BioPACE – Biometric passwords for next generation authentication protocols for machine-readable travel documents. *Datenschutz und Datensicherheit - DuD*, 37(6):363 – 366, 2013.

[EU04] EU. Integration of biometric features in passports and travel documents - regulation (EC) 2252/2004, 2004.

[EU05] EU. Commission Decision C(2005)409, 2005.

[ICA06] ICAO. *Doc 9303 Part 1 Machine Readable Passports Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability*. International Civil Aviation Organization (ICAO), 6 edition, 2006.

[ICA13] ICAO. *SUPPLEMENT to Doc 9303*. International Civil Aviation Organization (ICAO), 12 edition, 2013.

[IEE90] IEEE Std 610.12-1990 – Glossary of Software Engineering Terminology, 1990.

[ISO05] ISO/IEC TR 19759:2005 – Software Engineering – Guide to the Software Engineering Body of Knowledge (SWEBOK), 9 2005.

[ISO06a] ISO/IEC JTC 1/SC 31 - Automatic identification and data capture techniques. Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification. ISO/IEC 16022:2006, 2006.

[ISO06b] ISO/IEC JTC 1/SC 31 - Automatic identification and data capture techniques. Information Technology – Automatic Identification and Data Capture Techniques – QR Code 2005 Bar Code Symbology Specification. ISO/IEC 18004:2006, 2006.

[ISO11] ISO/IEC JTC 1/SC 27 - Security Techniques. Information Technology – Security Techniques – Biometric Information Protection. ISO/IEC 24745:2011, 2011.

[KN07] Dennis Kügler and Ingo Naumann. Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass. *Datenschutz und Datensicherheit - DuD*, 31(3):176–180, 2007.

[SB08] Walter Scheirer and Terrance Boult. Bio-cryptographic protocols with bipartite biotokens. In *Biometrics Symposium*, pages 9–16, 2008.

[SBB10] Walter Scheirer, Bill Bishop, and Terrance Boult. Beyond PKI: The Biocryptographic Key Infrastructure. In *Workshop Information Forensics and Security*, pages 1–6. IEEE, 2010.